УДК 519.21:004.056.53

Поперешняк С.В.

СУМІСНІСТЬ НЕОДНОРІДНОЇ СИСТЕМИ ЛІНІЙНИХ ВИПАДКОВИХ БУЛЕВИХ РІВНЯНЬ

Вступ

Нині у світі відбувається активний розвиток електронної комерції. При розробці систем електронної комерції фактор безпеки грає первинну роль. При цьому типовим завданням є створення системи роботи з партнерами, що надає захищений доступ до динамічно обновлюваної інформації.

Одним з ефективних способів створення підсистеми захисту в системах електронної комерції на сьогодні являється застосування криптографічних методів захисту інформації. Основу більшості криптографічних методів складають симетричні алгоритми шифрування, які прийнято підрозділяти на блокові і потокові. Швидкість роботи потокових алгоритмів зазвичай значно перевищує швидкість роботи блокових.

Оскільки Інтернет технології вимагають високих швидкостей, то одним з актуальних завдань в криптографії є розробка і реалізація високошвидкісних потокових алгоритмів шифрування, що програмно реалізовуються, забезпечують високу надійність захисту інформації, з хорошими технічними і експлуатаційними властивостями. До теперішнього часу значна частина запропонованих у відкритій літературі потокових шифрів заснована на регістрах зрушення над полем GF(2).

Випадкові матриці над скінченним полем та системи рівнянь з випадковою матрицею коефіцієнтів досліджувалися за різних умов в роботах Slepian D. (1955), Erdös P., Renyi A.(1963), Коваленка І.М. (1965, 1975), Козлова М.В.(1966), Балакіна Г.В. (1968, 1998), Левитської А.О.(1986), Колчіна В.Ф. (1997, 2000), Cooper C. (2000, 2001) та інших авторів.

Постановка задачі.

Нехай задана матриця A, $A=\|a_{ij}\|$, над полем $GF(2)$, що складається з двох елементів з відомим розподілом незалежних випадкових величин a_{ij}, $i=\overline{1,T}$, $j=\overline{1,n}$, $T/n/$ - число рядків /стовпців/ матриці A. Розглянемо неоднорідну систему лінійних рівнянь з матрицею коефіцієнтів A

$$AX=B, \qquad (1)$$

де вектор-стовпець $B=\begin{pmatrix} b_1 \\ . \\ . \\ b_T \end{pmatrix}$ не залежить від A, випадкові величини $b_1,...,b_T$ незалежні та приймають значення 0 і 1 з відомим розподілом, $X=\begin{pmatrix} x_1 \\ x_2 \\ . \\ . \\ x_n \end{pmatrix}$ - n-вимірний вектор-стовпець невідомих величин.

В роботах [1] - [3] різними методами досліджено граничну поведінку сумісності системи (1), коли $T=T(n)$ і $n\to\infty$. Зокрема, в [1, теорема 3.3.3] розглянуто це питання за умови, що незалежні випадкові величини a_{ij}, $i=\overline{1,T}$, $j=\overline{1,n}$ однаково розподілені.

Нас цікавлять оцінки ймовірності того, що вихідна система (1) має розв'язок, тобто є сумісна. Підгрунтям для доведення основних результатів роботи (теорема 1.1, теорема 1.2) слугують теореми статті [4]. Зазначимо також, що на відміну від [1], в даній роботі

розглядається випадкова матриця A, розподіли елементів якої можуть залежати від місць їх (елементів) розташування.

Основний результат

Розглянемо систему лінійних рівнянь $AX = B$ з матрицею коефіцієнтів A, де елементи $T \times n$ матриці $A = \|a_{ij}\|$ незалежні випадкові величини і для $i = \overline{1,T}$, $j = \overline{1,n}$

$$P\{a_{ij} = 1\} = 1 - P\{a_{ij} = 0\} = \frac{\ln n + x_{ij}}{n}, \tag{2}$$

де

$$|x_{ij}| \le c,\ c = const,\ i = \overline{1,T},\ j = \overline{1,n}. \tag{3}$$

Вектор-стовпець $B = \begin{pmatrix} b_1 \\ \cdot \\ \cdot \\ b_T \end{pmatrix}$ не залежить від A, випадкові величини $b_1, \ldots, b_T$ незалежні та приймають значення 0 і 1 з ймовірностями

$$P\{b_i = 0\} = \frac{1}{2}\left(1 + \varepsilon_i(n)\right),\ i = 1, 2, \ldots, T. \tag{4}$$

Позначимо $P_{n,T}$ ймовірність того, що система (1) є сумісною системою.

Теорема 1.1. *Нехай для усіх* $n \ge n_0 > 1$ $0 < \frac{T}{n} \le 1 - \frac{\log_2 \ln n}{(\ln n)^q}$, $q = const$, $0 < q < 1$, *і виконуються умови (2) та*

$$\tilde{\varepsilon}(n) \le \beta < 1,\ \beta = const. \tag{5}$$

де

$$\tilde{\varepsilon}(n) = \max_{1 \le k \le T} |\varepsilon_k(n)|. \tag{6}$$

Тоді має місце

$$-\alpha_2 f(n) - \tilde{\varepsilon}(n) \le P_{n,T} - e^{-\lambda/2} \le \alpha_1 f(n) + \tilde{\varepsilon}(n), \tag{7}$$

де $f(n) = 4(1+\delta)e^{e^c}\frac{\ln^4 n}{n(\ln\ln n)^2}$, $\alpha_1 = 1 + \frac{1}{1 - \tilde{\varepsilon}(n)}$, $\alpha_2 = 1 + \Delta(n) + \frac{1}{1 + \tilde{\varepsilon}(n)}$, $\lambda = \frac{1}{n}\sum_{i=1}^{T} \exp\left\{-\frac{1}{n}\sum_{j=1}^{n} x_{ij}\right\}$,
$\delta > 0$, $\delta = const$, $\Delta(n) \to 0$ *при* $n \to \infty$.

Далі припустимо, що

$$P\{a_{ij} = 1\} = 1 - P\{a_{ij} = 0\} = \frac{\ln T + x_{ij}}{T}, \tag{8}$$

де x_{ij} задовольняє умову (3). Покладемо

$$P\{b_i = 0\} = \frac{1}{2}\left(1 + \varepsilon_i(T)\right),\ i = 1, 2, \ldots, T. \tag{9}$$

Нехай також

$$\lambda_1 = \frac{1}{T}\sum_{i=1}^{n} \exp\left\{-\frac{1}{T}\sum_{j=1}^{T} x_{ij}\right\}.$$

Теорема 1.2. *Нехай для усіх* $n \ge n_0 > 1$ $1 + \frac{\log_2 \ln n}{(\ln n)^q} \le \frac{T}{n} < \infty$, $q = const$, $0 < q < 1$, *і виконуються умови (3), (8)-(9) та*

$$\widetilde{\varepsilon}(T) \le \gamma < 1,\ \gamma = const, \qquad (10)$$

де $\max\limits_{1\le k\le n}\left|\varepsilon_k(T)\right| = \widetilde{\varepsilon}(T)$.

Тоді має місце

$$-\alpha_2^* f(T) - \widetilde{\varepsilon}(T) \le P_{n,T} - e^{-\lambda_1/2} \le \alpha_1^* f(T) + \widetilde{\varepsilon}(T),$$

де $f(T) = 4(1+\delta)e^{e^c}\dfrac{\ln^4 T}{T(\ln\ln T)^2}$, $\alpha_1^* = 1 + \dfrac{1}{1-\widetilde{\varepsilon}(T)}$, $\alpha_2^* = 1 + \Delta(T) + \dfrac{1}{1+\widetilde{\varepsilon}(T)}$, $\Delta(T) \to 0$ *при* $T \to \infty$.

Допоміжні твердження

Будемо вважати, що матриця A має принаймні n_1 стовпців так, що для $n \ge n_1$ задання розподілів (2) є коректним.

Позначимо $r(A)$ ранг матриці A.

Теорема 2.1. *Нехай мають місце умови (2), (3) і для* $n > n_0$ *виконується* $0 < \dfrac{T}{n} \le 1 - \dfrac{\log_2 \ln n}{(\ln n)^q}$, $q = const$, $0 < q < 1$. *Тоді для к, к=0,1,2,...,*

$$\left| P\{r(A) = T - k\} - \frac{e^{-\lambda}\cdot\lambda^k}{k!} \right| \le 2(1+\delta)c(n,k)\frac{\ln^4 n}{n(\ln\ln n)^2},$$

де $1 < \underline{\lim\limits_{n\to\infty}} c(n,k) \le \overline{\lim\limits_{n\to\infty}} c(n,k) \le e^{e^c}$, $\delta > 0$, $\delta = const$.

Доведення теореми 2.1 приведено в [4].

Теорема 2.2. *Нехай мають місце умови (3),(8) і для* $n > n_0$ *виконується* $1 + \dfrac{\log_2 \ln n}{(\ln n)^q} \le \dfrac{T}{n} < \infty$, $q = const$, $0 < q < 1$. *Тоді для к, к=0,1,2,...,*

$$\left| P\{r(A) = n - k\} - \frac{e^{-\lambda_1}\cdot\lambda_1^k}{k!} \right| \le 2(1+\delta)c(T,k)\frac{\ln^4 T}{T(\ln\ln T)^2},$$

де $1 < \underline{\lim\limits_{n\to\infty}} c(T,k) \le \overline{\lim\limits_{n\to\infty}} c(T,k) \le e^{e^c}$, $\delta > 0$, $\delta = const$.

Доведення теореми 2.2. аналогічно доведенню теореми 2.1.

Доведення теореми 1.1

Позначимо $\mu_{n,T}$ число розв'язків системи (1). Ймовірність $P_{n,T}$ сумісності системи (1) – це ймовірність того, що система має хоча б один розв'язок, тобто $P_{n,T} = \mathrm{P}\{\mu_{n,T} > 0\}$.

Знайдемо явний вигляд ймовірності події $\{\mu_{n,T} > 0\}$ за умови, що ранг $r(A)$ матриці A дорівнює r. З цією метою будемо вважати (не порушуючи загальності), що в матриці A лінійно незалежними є рядки з номерами 1,2, . . . ,r. Тоді кожен з рядків з номерами r+1, . . ., T , буде лінійною комбінацією перших r рядків, і для того, щоб система була сумісна, праві частини $b_{r+1}, \ldots, b_T$ повинні задовольняти співвідношенням вигляду

$$\varepsilon_{1i}^* b_1 \oplus \ldots \oplus \varepsilon_{ri}^* b_r = b_i,\ i = r+1, \ldots, T, \qquad (11)$$

де $\varepsilon_{1i}^*, \ldots, \varepsilon_{ri}^*$ приймають значення 0 або 1, $\oplus$ - знак додавання у полі $GF(2)$.

Ймовірність одного довільного із співвідношень (11) дорівнює

$$\mathrm{P}\left\{b_{\nu_1}\oplus\ldots\oplus b_{\nu_s}=b_i\right\}=\frac{1}{2}\left(1+\left(\prod_{j=1}^{s(i)}\varepsilon_{\nu_j}(n)\right)\varepsilon_i(n)\right),\qquad(12)$$

де $1\le s\le r,\ s=s(i), i=r+1,\ldots,T$, $s(i)$ - це кількість ненульових доданків в лівій частині (11), сума яких дає нам значення b_i. В справедливості рівності (12) можна переконатися за допомогою методу повної математичної індукції.

Використовуючи (12), отримуємо, очевидно, співвідношення

$$\mathrm{P}\left\{\mu_{n,T}>0\,\middle|\,r(A)=r\right\}=\frac{1}{2^{T-r}}\prod_{i=r+1}^{T}\left(1+\left(\prod_{j=1}^{s(i)}\varepsilon_j(n)\right)\varepsilon_i(n)\right).$$

Оскільки $r(A)=r$, то враховуючи теорему 3.1.1 [1] згідно з якою $r+k=T$, де k - максимальне число незалежних критичних наборів, маємо

$$P_{n,T}=\sum_{r=0}^{T}\mathrm{P}\{r(A)=r\}\frac{1}{2^{T-r}}\prod_{i=r+1}^{T}\left(1+\left(\prod_{j=1}^{s(i)}\varepsilon_j(n)\right)\varepsilon_i(n)\right)=\sum_{r=0}^{T}\mathrm{P}\{r(A)=T-k\}\frac{1}{2^k}\prod_{i=r+1}^{T}\left(1+\left(\prod_{j=1}^{s(i)}\varepsilon_j(n)\right)\varepsilon_i(n)\right).$$

Звідси, приймаючи до уваги позначення (6), отримуємо

$$\sum_{k=0}^{T}\mathrm{P}\{r(A)=T-k\}\left(\frac{1-\tilde{\varepsilon}(n)}{2}\right)^k\le P_{n,T}\le\sum_{k=0}^{T}\mathrm{P}\{r(A)=T-k\}\left(\frac{1+\tilde{\varepsilon}(n)}{2}\right)^k.\qquad(13)$$

Далі покажемо, що

$$P_{n,T}-e^{-\lambda/2}\le\alpha_1 f(n)+\tilde{\varepsilon}(n).\qquad(14)$$

Дійсно, оцінимо зверху різницю $P_{n,T}-e^{-\lambda/2}$, використавши праву частину співвідношення (13)

$$P_{n,T}-e^{-\lambda/2}\le\sum_{k=0}^{T}P\{r(A)=T-k\}\left(\frac{1+\tilde{\varepsilon}(n)}{2}\right)^k-e^{-\lambda/2}=$$

$$=\sum_{k=0}^{T}\left[P\{r(A)=T-k\}-\frac{e^{-\lambda}\lambda^k}{k!}\right]\frac{1}{2^k}+\sum_{k=0}^{T}\frac{e^{-\lambda}\lambda^k}{k!}\frac{1}{2^k}-e^{-\lambda/2}+\theta,$$

де $\theta=\left\langle\sum_{k=0}^{T}\left[P\{r(A)=T-k\}-\frac{e^{-\lambda}\lambda^k}{k!}\right]+\sum_{k=0}^{T}\frac{e^{-\lambda}\lambda^k}{k!}\right\rangle\frac{(1+\tilde{\varepsilon}(n))^k-1}{2^k}$.

Скориставшись теоремою 2.1, отримаємо

$$P_{n,T}-e^{-\lambda/2}\le f(n)+\theta.\qquad(15)$$

Оцінимо суму θ зверху, знову скориставшись теоремою 2.1,

$$\theta\le\frac{f(n)}{2}\sum_{k=0}^{T}\frac{(1+\tilde{\varepsilon}(n))^k-1}{2^k}+e^{-\lambda}\sum_{k=0}^{T}\frac{\lambda^k}{k!}\frac{(1+\tilde{\varepsilon}(n))^k-1}{2^k}\le\frac{f(n)}{2}\sum_{k=0}^{T}\frac{(1+\tilde{\varepsilon}(n))^k}{2^k}+e^{-\lambda}\sum_{k=0}^{T}\frac{\lambda^k}{k!}\frac{\tilde{\varepsilon}(n)2^k}{2^k}.$$

Звідси

$$\theta\le\frac{f(n)}{2}\frac{1}{1-\frac{1+\tilde{\varepsilon}(n)}{2}}+\tilde{\varepsilon}(n).\qquad(16)$$

З (15) та (16) випливає (14).

Покажемо, що

$$P_{n,T} - e^{-\lambda/2} \geq -\alpha_2 f(n) - \tilde{\varepsilon}(n). \qquad (17)$$

Дійсно, оцінимо знизу різницю $P_{n,T} - e^{-\lambda/2}$, використавши ліву частину співвідношення (13),

$$P_{n,T} - e^{-\lambda/2} \geq \sum_{k=0}^{T} P\{r(A) = T-k\}\left(\frac{1-\tilde{\varepsilon}(n)}{2}\right)^k - e^{-\lambda/2} =$$

$$= \sum_{k=0}^{T}\left[P\{r(A) = T-k\} - \frac{e^{-\lambda}\lambda^k}{k!}\right]\frac{1}{2^k} + \sum_{k=0}^{T}\frac{e^{-\lambda}\lambda^k}{k!}\frac{1}{2^k} - e^{-\lambda/2} + \theta,$$

де $\theta = \left\langle \sum_{k=0}^{T}\left[P\{r(A) = T-k\} - \frac{e^{-\lambda}\lambda^k}{k!}\right] + \sum_{k=0}^{T}\frac{e^{-\lambda}\lambda^k}{k!}\right\rangle \frac{(1-\tilde{\varepsilon}(n))^k - 1}{2^k}$.

Скориставшись теоремою 2.1, отримаємо $P_{n,T} - e^{-\lambda/2} \geq -f(n) + \sum_{k=0}^{T}\frac{e^{-\lambda}\lambda^k}{k!}\frac{1}{2^k} - e^{-\lambda/2} + \theta$.

Звідси

$$P_{n,T} - e^{-\lambda/2} \geq -f(n) + \sum_{k=0}^{\infty}\frac{e^{-\lambda}\left(\lambda/2\right)^k}{k!} - \sum_{k=T+1}^{\infty}\frac{e^{-\lambda}\left(\lambda/2\right)^k}{k!} - e^{-\lambda/2} + \theta = -f(n) - \sum_{k=T+1}^{\infty}\frac{e^{-\lambda}\left(\lambda/2\right)^k}{k!} + \theta$$

$$\geq -f(n) - e^{-\lambda}\sum_{k=T+1}^{\infty}\left(\frac{\lambda e}{2k}\right)^k \frac{1}{\sqrt{2\pi k}} + \theta.$$

Беручи до уваги те, що $\frac{\lambda e}{2T} < 1$, отримаємо

$$P_{n,T} - e^{-\lambda/2} \geq -f(n)(1 + \Delta(n)) + \theta, \qquad (18)$$

де

$$0 \leq \Delta(n) \leq \left(\frac{\lambda e}{2T}\right)^{T+1}\frac{\sqrt{2T}}{2T - \lambda e}(f(n))^{-1}. \qquad (19)$$

Оцінимо суму θ знизу, знову скориставшись теоремою 2.1,

$$\theta \geq -\frac{f(n)}{2}\sum_{k=0}^{T}\frac{(1-\tilde{\varepsilon}(n))^k - 1}{2^k} + e^{-\lambda}\sum_{k=0}^{T}\frac{\lambda^k}{k!}\frac{(1-\tilde{\varepsilon}(n))^k - 1}{2^k} \geq -\frac{f(n)}{2}\sum_{k=0}^{T}\frac{(1-\tilde{\varepsilon}(n))^k}{2^k} - e^{-\lambda}\sum_{k=0}^{T}\frac{\lambda^k}{k!}\frac{\tilde{\varepsilon}(n)2^k}{2^k}.$$

Звідси

$$\theta \geq -\frac{f(n)}{2}\frac{1}{1 - \frac{1-\tilde{\varepsilon}(n)}{2}} - \tilde{\varepsilon}(n). \qquad (20)$$

Із (18) за допомогою (19), (20) отримуємо (17).

З (14) та (17) випливає співвідношення (7). Теорема 1.1 доведена.

Доведення теореми 1.2

Доведення теореми 1.2 можна виконати аналогічно доведенню теореми 1.1, скориставшись при цьому теоремою 2.2.

Асимптотика ймовірності $P_{n,T}$

Теорема 5.1. *Нехай виконуються умови теореми 1.1. та*

$$\lambda \to \lambda^* \qquad (21)$$

і

$$\widetilde{\varepsilon}(n) \to 0 \ \textit{при} \ n \to \infty . \qquad (22)$$

Тоді

$$0 < \lambda^* < \infty \qquad (23)$$

і має місце співвідношення

$$P_{n,T} \to e^{-\lambda^*/2} . \qquad (24)$$

Нерівність (23) встановлена в [1, теорема 2], а співвідношення (24), з урахуванням умов (21) і (22), безпосередньо випливає із теореми 1.1.

Наслідок 5.1. Якщо виконується умова (2), в якій $x_{ij} = x$, $i = \overline{1,T}$, $j = \overline{1,n}$, x - фіксоване число, і при $n \to \infty$ $T/n \to \alpha$, де $0 < \alpha < 1$, то має місце співвідношення (21), в якому $\lambda^* = \alpha e^{-x}$.

Теорема 5.2. *Нехай виконуються умови теореми 1.2. та* $\lambda_1 \to \lambda_1^*$ *і* $\widetilde{\varepsilon}(T) \to 0$ *при* $T \to \infty$. *Тоді* $0 < \lambda_1^* < \infty$ *і має місце співвідношення*

$$P_{n,T} \to e^{-\lambda_1^*/2} . \qquad (25)$$

Доведення теореми 5.2 аналогічне доведенню теореми 5.1.

Наслідок 5.2. Якщо виконується умова (8), в якій $x_{ij} = x$, $i = \overline{1,T}$, $j = \overline{1,n}$, x - фіксоване число, і при $n \to \infty$ $T/n \to \alpha$, де $1 < \alpha < \infty$, то має місце співвідношення (25), в якому $\lambda_1^* = \alpha^{-1} e^{-x}$.

Висновки

Прикладні аспекти теорії кодування інформації та захисту її від несанкціонованого доступу, теорії тестування генераторів псевдовипадкових чисел і теорії розпізнавання приводять до задач про сумісність лінійних випадкових булевих рівнянь.

У роботі знайдені верхня і нижня оцінки ймовірності того, що неоднорідна система лінійних випадкових булевих рівнянь має розв'язок (теорема 1.1, теорема 1.2). Зазначені теореми різняться між собою припущенням на відношення числа рядків та числа стовпців матриці коефіцієнтів. На основі цих теорем отримана асимптотика ймовірності сумісності системи (1). Наслідок 5.1 доведено також в [1, теорема 3.3.3].

Отримані результати представляють як теоретичний, так і практичний інтерес, зокрема, для задач кодування інформації при передачі її каналами зв'язку та захисту інформації від несанкціонованого доступу.

Список літератури

1. *Колчин В.Ф.,* Случайные графы. – М.: Физматлит, 2004. – 256 с.
2. *Коваленко И.Н.,* О теоремах инвариантности для случайных булевых матриц. // Кибернетика. – 1975. - №5. – С. 138-145.
3. *Балакин Г.В.,* Распределение ранга случайных матриц над конечным полем. // Теория вероятностей и её применения. – 1968. – в. XIII, №4. – С. 631-641.
4. *Поперешняк С.В.,* Про швидкість збliження розподілів рангу випадкової розрідженої матриці у полі $GF(2)$ та Пуассона. // Науковий журнал «Захист інформації». – К. Вид-во: ДУІКТ. -2010.- №3 – С. 94-100.

Рецензент: Прокопенко І.Г.
Надійшла 03.11.2010